netForensics®
The World Trusts Us

nFX™ Open Security Platform: Optimizing Security Operations

The nFX™ Open Security Platform (nFX OSP), netForensics' flagship Security Information Management (SIM) solution, is the industry's only solution built on a standards-based methodology to optimize security operations.

nFX OSP empowers the security organization with the agility required to meet the information security challenges facing today's enterprise by:

- Creating an auditable security infrastructure to demonstrate compliance with key regulatory statutes.
- Preventing catastrophic loss by protecting critical assets and identifying attacks quickly.
- Enabling analysts to conduct historical or "forensic" analysis when an attack occurs to determine the full extent and source of an attack.
- Reducing the risk baseline.
- Increasing the value of existing information security investments
- Improving the effectiveness of security personnel by increasing the efficiency of limited human resources and closing knowledge gaps.
- Measuring security operations performance against key metrics.

nFX OSP sets the standard for enterprise Security Information Management by providing customers with a completely integrated solution that meets the security team's requirements for real-time monitoring and historical analysis of security information. nFX OSP is the only SIM solution built on a robust enterprise class ***architecture*** that can scale to deliver 24x7 SIM across a complex, distributed, and heterogeneous enterprise. The nFX OSP architecture forms a backbone to guarantee users reliable access to rich SIM functionality including ***event normalization, comprehensive correlation, real-time notification, dynamic threat visualization, reporting and analytics, embedded security knowledge, incident resolution management, policy compliance,*** and ***vulnerability management.*** The end result is a flexible security infrastructure that helps the security organization prepare to combat, identify, and respond to threats to mitigate risk and continuously reduce time to remediation.

KEY POINTS

» Out-of-the-box device integration and custom connectivity for proprietary devices.

» N-tier architecture with multiple forms of redundancy to guarantee 24x7 availability without compromising performance.

» Operations reporting for performance measurement.

» Event normalization, aggregation, and comprehensive correlation to rationalize massive volumes of security events, speed identification, and eliminate false positives.

» Real-time monitoring and alerting including a fully customizable dashboard environment with multiple views to aid identification.

» Advanced data visualization with integrated reporting and analytics for complete forensic analysis.

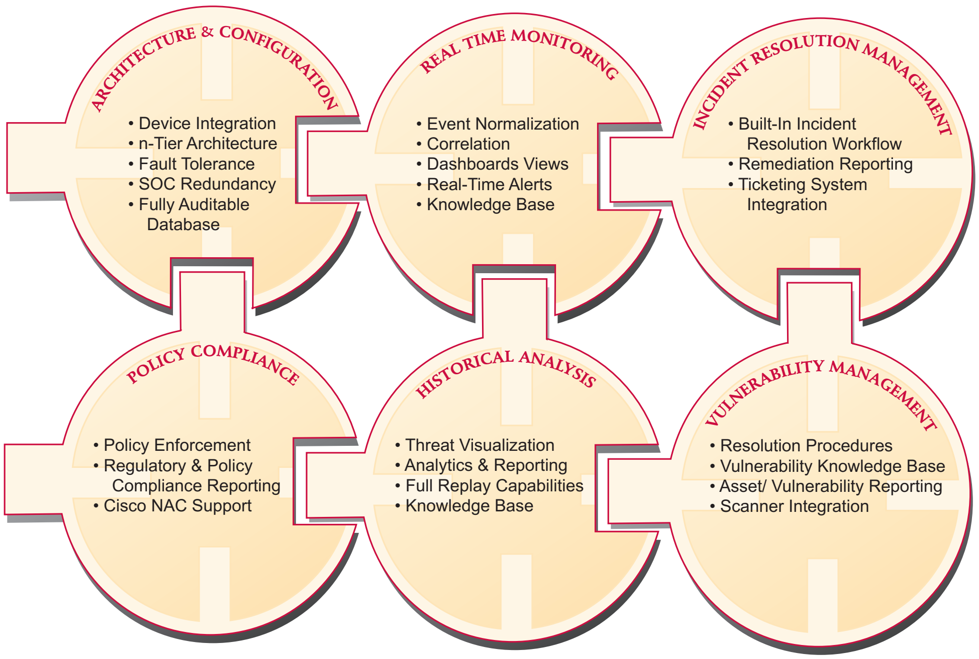
» Integrated knowledge base for unified access to the latest vulnerability information—including detailed remediation steps.

» Out-of-the-box remediation workflow based on an industry standards model to ensure that threats are effectively eliminated.

» Policy integration and reporting supporting Cisco's NAC initiative and major regulatory compliance initiatives.

» Key vulnerability management capabilities including scanner integration and vulnerability reporting.

nFX Open Security Platform



Architecture and Integration:

While the advanced functionality and usability of a SIM solution can transform the way a security organization works, it must be built on a scalable architecture for customers to realize its full value. The nFX Open Security Platform is built on the industry's most robust architecture to meet the performance demands of a mission critical infrastructure application running across multiple sites. This gives management the confidence it needs to know that the security operations center is up and running and protecting the enterprise, and that the data needed to comply with an audit remain available and uncompromised. The nFX OSP architecture includes the following capabilities:

DEVICE INTEGRATION—The nFX OSP integrates natively with hundreds of network and security devices and applications including Intrusion Detection Systems, Firewalls, Operating Systems, and Anti-Virus Systems. The nFX Open security platform connects to most devices out of the box, and most importantly—these connections don't require installation on the actual devices themselves, and can be administered centrally. In rare instances when a device isn't natively supported, nFX OSP allows users to create custom connections via an easy-to-use API.

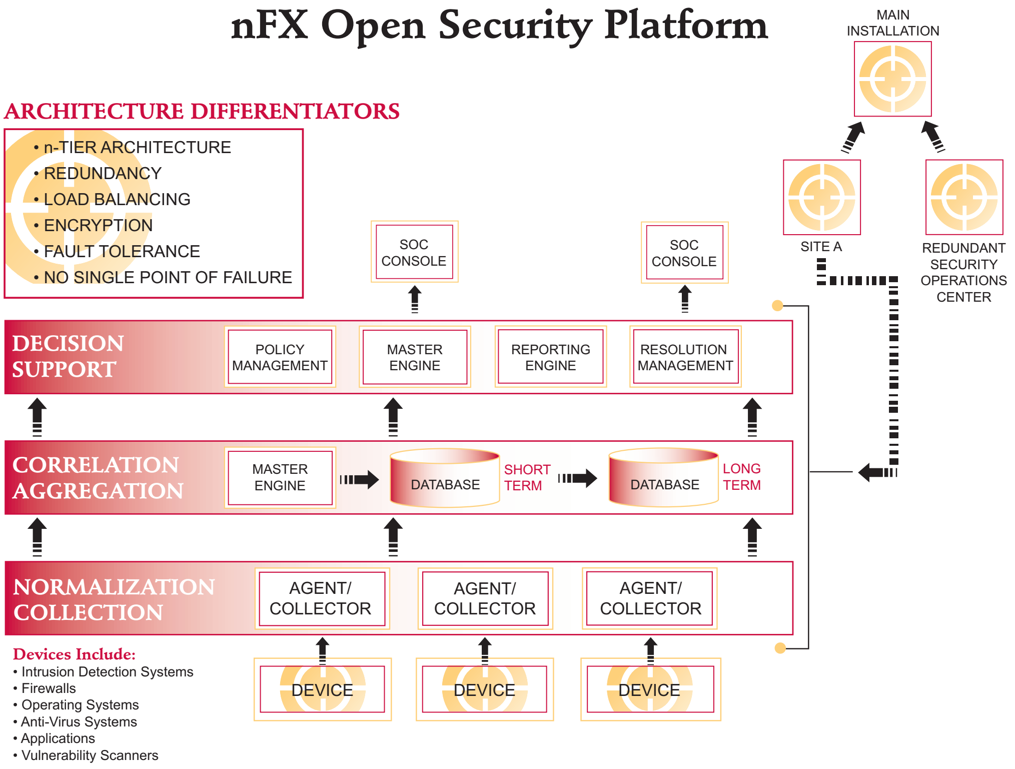
N-TIER ARCHITECTURE—The nFX OSP architecture is fully federated for high performance and scalability across any network, regardless of how many locations are involved in an implementation. This ensures that there is no single point of failure, and that the application can be efficiently distributed to optimize performance based on users and event volume; the multi-tier architecture also allows organizations to minimize hardware requirements and easily expand the SIM infrastructure as business requirements change without performance degradation.

FAULT TOLERANCE AND LOAD SHARING—Multiple forms of failover guarantee that the nFX Open Security Platform will be up and running regardless of how large or small the enterprise infrastructure is. Customers can create redundancy at every level of the SIM architecture within one site or across a distributed installation. nFX OSP provides agent collector to engine, engine to engine, and database to database failover to create redundancy across a distributed SIM implementation. This provides an important alternative to SIM solutions that rely on a single point of failure, and ensures that operators have continuous access to real time and historical security information. These multiple redundancy options make it easier and more cost effective for security organizations to deploy a back up SOC that is based on actual business requirements. For example, if an organization has the network resources to create redundancy at the event level for compliance purposes, they can. Or if they just need to replace correlated data in the event of an outage, nFX OSP supports this level of redundancy as well.

SELF HEALING ADMINISTRATION—nFX OSP is the only SIM solution available today with a built in health module to continuously monitor the implementation and report on problems when they occur. The product can automatically make certain modifications to improve performance. nFX OSP also integrates with HP OpenView™ to connect SIM to the network systems management infrastructure.

FULLY AUDITABLE DATABASE—The nFX Open Security Platform uses a robust, yet flexible data architecture to maintain the integrity of data over time to support compliance, audit, and operational reporting requirements. Customers have multiple options for distributing and archiving stored data. The open data architecture also allows nFX OSP data to be easily leveraged by other applications.

nFX Open Security Platform

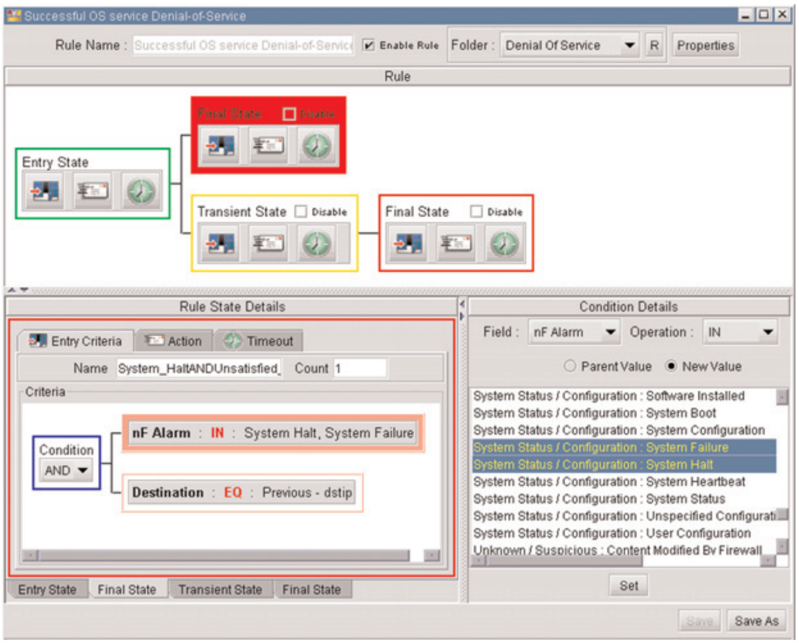


Normalization, Correlation, and Real-Time Notification

The nFX Open Security Platform improves the efficiency and responsiveness of the security organization by aggregating and normalizing large volumes of diverse security events, automatically correlating them against threat and asset value to separate real threats from false positives, and presenting analysts with a prioritized list of events. nFX OSP also supports real-time notification of key staff when a high risk threat is identified. nFX OSP contains the following functionality for normalization, correlation and real-time notification:

EVENT AGGREGATION & NORMALIZATION—nFX OSP automatically aggregates events from thousands of disparate sources into a single data format, and then normalizes them into a manageable number of 100 event types across 9 categories. This makes it possible to automatically identify events using correlation, generate reports, and perform analysis from a meaningful data set.

COMPREHENSIVE CORRELATION— netForensics is the only Security Information Management vendor to integrate statistical, rules based, and vulnerability correlation to speed threat identification and reducing risk by providing a true picture of risk based on business impact. By combining all three types of correlation with asset valuation, netForensics provides security analysts with a true risk profile for each event, while reducing the organization's total risk exposure over time.



Successful OS service Denial-of-Service

Rule Name : Successful OS service Denial-of-Service ☑ Enable Rule Folder : Denial Of Service

Name System_HaltANDUnsatisfied_ Count 1

Condition AND

nF Alarm : IN : System Halt, System Failure

Destination : EQ : Previous - dstip

Field : nF Alarm Operation : IN

○ Parent Value ● New Value

System Status / Configuration : Software Installed
System Status / Configuration : System Boot
System Status / Configuration : System Configuration
System Status / Configuration : System Failure
System Status / Configuration : System Halt
System Status / Configuration : System Heartbeat
System Status / Configuration : System Status
System Status / Configuration : Unspecified Configurati
System Status / Configuration : User Configuration
Unknown / Suspicious : Content Modified By Firewall

The nFX Open Security Platform provides a multi-state rules correlation engine that allows a rule to run long enough to meet multiple conditions before an alert is issued, reducing the number of false positives.

- nFX OSP applies statistical algorithms out-of-the-box to automatically determine incident severity and then assigns a threat score based on asset value. This statistical correlation analyzes network behavior and identifies threat based on the presence and severity of anomalous event patterns. In addition to giving security analysts a way to identify threats without any configuration, nFX OSP data can be used to measure effectiveness by determining whether the number of attack patterns against high value assets has decreased over time.

- nFX OSP rules-based correlation allows users to apply conditional logic to identify likely attack scenarios by observing a specific series of events within a specified amount of time. The nFX Open Security Platform is the only SIM solution that lets security personnel deploy and modify pre-existing event correlation rules or develop custom rules with multiple states to improve threat identification and reduce false positives.
- nFX OSP combines support for long-running rules with an intuitive rules development GUI to make it easy for users to define, modify, and deploy robust rules.
- nFX OSP correlates IDS data with multiple sources of vulnerability data—including data from vulnerability management scanners and a database of known vulnerabilities—and assigns a confidence level to those events which are not readily determined to be false positives or false alarms. That data is then correlated against asset threat data and a risk score is assigned to each asset, allowing security operators to see the business impact of specific events. Security operators can then assess in real-time whether action should be taken based on the likelihood that an event could take advantage of vulnerability in a particular asset, the asset's susceptibility to that vulnerability, and the asset's value.
- Unlike other SIM products, the nFX Open Security Platform is the only solution on the market that supports vulnerability correlation *without writing rules*. This means that security teams can immediately reap the benefits of vulnerability correlation, and don't have to lose time writing and maintaining rules to get the most valuable method of identifying attacks in place.

REAL-TIME EVENT NOTIFICATION—When a high priority threat is identified by the system, analysts receive notification by their preferred method—email, pager, fax, etc. Reports can also be scheduled to run on a set basis.This is especially important for organizations that can't fully fund a 24x7 security operations center.

Embedded Security Knowledge

nFX OSP provides analysts with instant access to the netForensics knowledge base, eliminating the need to perform hours of research from a variety of external sources on vulnerabilities and threats. The knowledge base is integrated with all of the functional areas of the nFX Open Security Platform to ensure that vulnerability information, compliance guidelines, and remediation procedures are never more than a click away.

INTEGRATED KNOWLEDGE BASE—

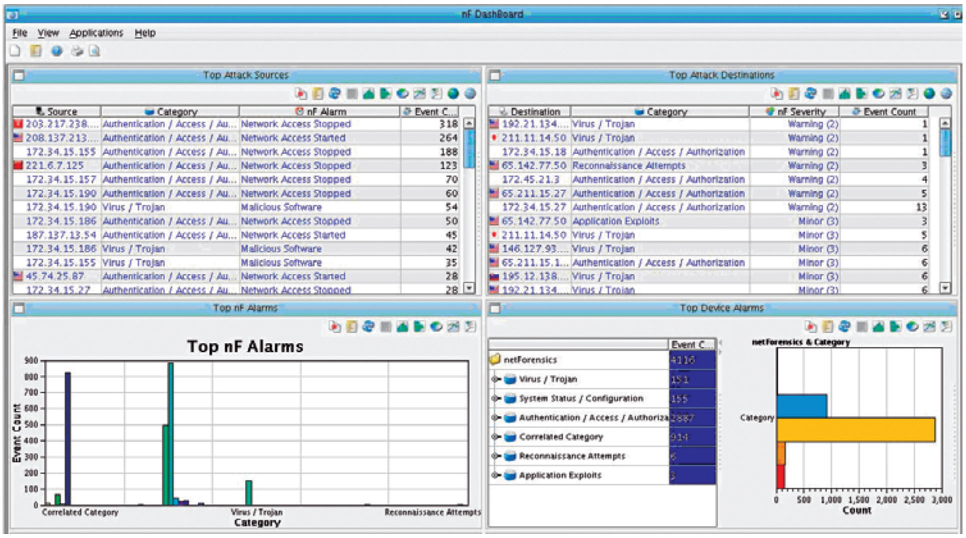
- The knowledge base contains information on a range of issues, including newly discovered vulnerabilities, malware, and vendor-specific vulnerability data directly from the nFX Open Security Platform.
- netForensics is the only SIM vendor with a dedicated research team that publishes regular knowledge base advisories to help security teams keep pace with the burgeoning volume of vulnerability information. These advisories include advice on how to tune nFX OSP to recognize and react to events when they occur.
- Customers receive dynamic updates directly from the Web to make sure that the knowledge base is fully updated with the latest information.

Analytics & Reporting

It's impossible to manage what can't be measured, and it's equally difficult for security personnel to take action without information. The nFX Open Security Platform allows users to run a wide range of reports and then perform detailed ad-hoc analysis to get the answers they need:

FLEXIBLE REPORTING—The nFX Open Security Platform creates a rich reporting environment that allows security teams to generate reports that incorporate real-time and historical data to measure security operations performance, compliance, and emerging threats. Reports are seamlessly integrated with analytics and data visualization views to provide a comprehensive understanding of an organization's security picture at any point in time. nFX OSP provides the following reporting capabilities:

- More than 250 out of the box reports measure everything from performance against key indicators like time to remediation and risk exposure, to compliance with regulatory statutes. Tactical reports show case status or threats affecting different assets.
- Custom report creation gives users tailored report information relevant to their specific enterprise security processes and procedures.
- Role-based dashboards meet the specific information needs of analysts, operators and executives out of the box. These fully customizable dashboards support multiple layout formats, while allowing users to combine real-time and historical views of information.



Top Attack Sources

Source	Category	nF Alarm	Event C...
203.217.238....	Authentication / Access / Au...	Network Access Stopped	318
208.137.213....	Authentication / Access / Au...	Network Access Started	264
172.34.15.155	Authentication / Access / Au...	Network Access Stopped	188
221.6.7.125	Authentication / Access / Au...	Network Access Stopped	123
172.34.15.157	Authentication / Access / Au...	Network Access Stopped	70
172.34.15.190	Authentication / Access / Au...	Network Access Stopped	60
172.34.15.190	Virus / Trojan	Malicious Software	54
172.34.15.186	Authentication / Access / Au...	Network Access Stopped	50
187.137.13.54	Authentication / Access / Au...	Network Access Started	45
172.34.15.186	Virus / Trojan	Malicious Software	42
172.34.15.155	Virus / Trojan	Malicious Software	35
45.74.25.87	Authentication / Access / Au...	Network Access Started	28
172.34.15.27	Authentication / Access / Au...	Network Access Stopped	28

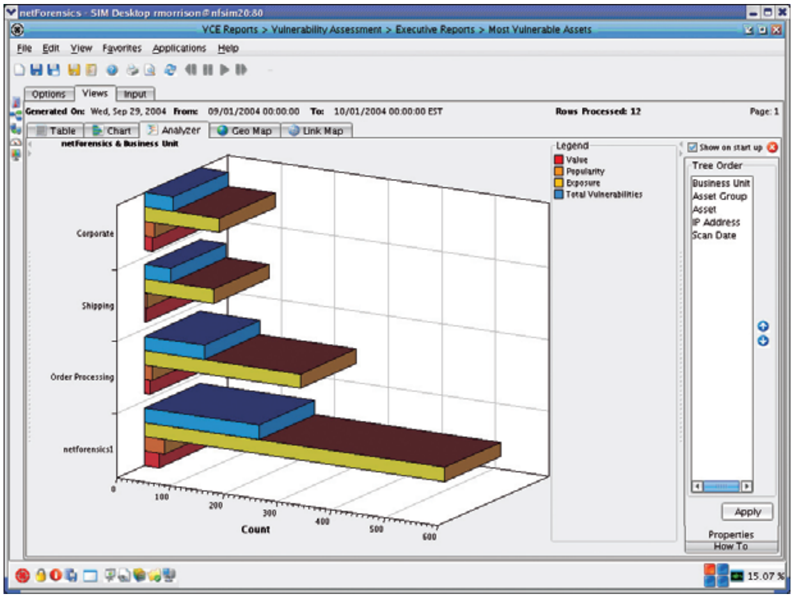
Top Attack Destinations

Destination	Category	nF Severity	Event Count
192.21.134....	Virus / Trojan	Warning (2)	1
211.11.14.50	Virus / Trojan	Warning (2)	1
172.34.15.18	Authentication / Access / Authorization	Warning (2)	1
65.142.77.50	Reconnaissance Attempts	Warning (2)	3
172.45.21.3	Authentication / Access / Authorization	Warning (2)	4
65.211.15.27	Authentication / Access / Authorization	Warning (2)	5
172.34.15.27	Authentication / Access / Authorization	Warning (2)	13
65.142.77.50	Application Exploits	Minor (3)	3
211.11.14.50	Virus / Trojan	Minor (3)	5
146.127.93....	Virus / Trojan	Minor (3)	6
65.211.15.1...	Authentication / Access / Authorization	Minor (3)	6
195.12.138....	Virus / Trojan	Minor (3)	6
192.21.134....	Virus / Trojan	Minor (3)	6

Top Device Alarms

	Event C...
netForensics	4116
Virus / Trojan	151
System Status / Configuration	155
Authentication / Access / Authoriza	2887
Correlated Category	914
Reconnaissance Attempts	6
Application Exploits	3

The nFX Open Security Platform contains an integrated dashboard so analysts and operators can get immediate access to their key operational metrics including top source destinations, top alarms, vulnerabilities by host, and incident cases that are open or closed.



Generated On: Wed, Sep 29, 2004 From: 09/01/2004 00:00:00 To: 10/01/2004 00:00:00 EST Rows Processed: 12 Page: 1

The nFX Open Security Platform makes it easy for executives to measure performance against key operational metrics, including time to resolution and compliance with security policy as it pertains to regulatory compliance. In this case, an executive gets an overall picture of risk exposure based on business unit.

POWERFUL ANALYTICS WITH INTEGRATED CHARTING—nFX OSP contains powerful next generation analytics that allow users to slice and dice security data using multiple dimensions of data in a familiar pivot table format:

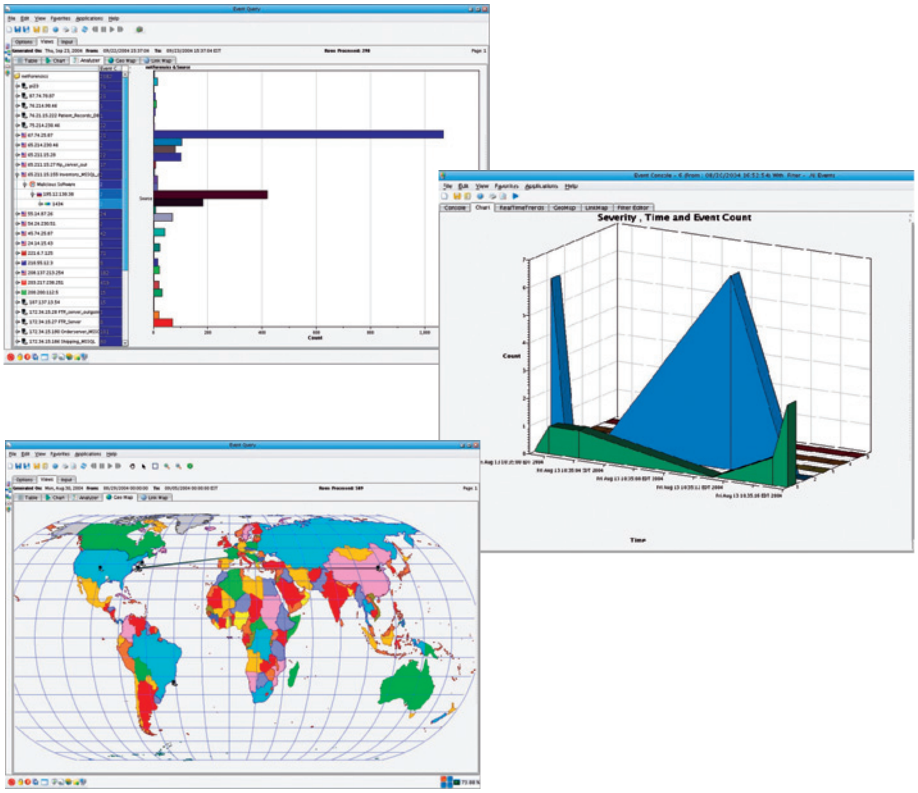
- Data mining functionality helps security personnel to analyze events based on specific criteria to identify anomalous incidents. As a result, security analysts can pinpoint raw event details that were previously undetectable in a console style view.
- Drillable charts present the results in an intuitive format while allowing further analysis.
- Analysts gain detailed views of specific actions over any given time period.

Advanced Threat Visualization

netForensics nFX Open Security Platform is the first SIM solution that allows companies to use visual tools on top of tabular reports and sophisticated analytics to assimilate information faster, differentiate false positives from real threats, understand the exact nature and scope of a threat, and make sure that vulnerabilities are mitigated before a threat can proliferate. The nFX Open Security Platform delivers a comprehensive range of visual tools to help security practitioners rationalize the large number of security events created in today's business climate:

EXPERT ASSISTANT—Guides users through the different views to quickly get the information they need to identify and analyze threats based on attack type.

THE LINK MAP—Allows analysts to visualize relationships among different assets under attack to identify the target, type and method of attack. Analysts can immediately see the course of an attack in real-time as it propagates across a network. Playback controls let users recreate the attack so they can determine the full extent of vulnerabilities and anticipate where an attack is heading. Analysts can then drill down on a specific asset at any time to get more specific information.



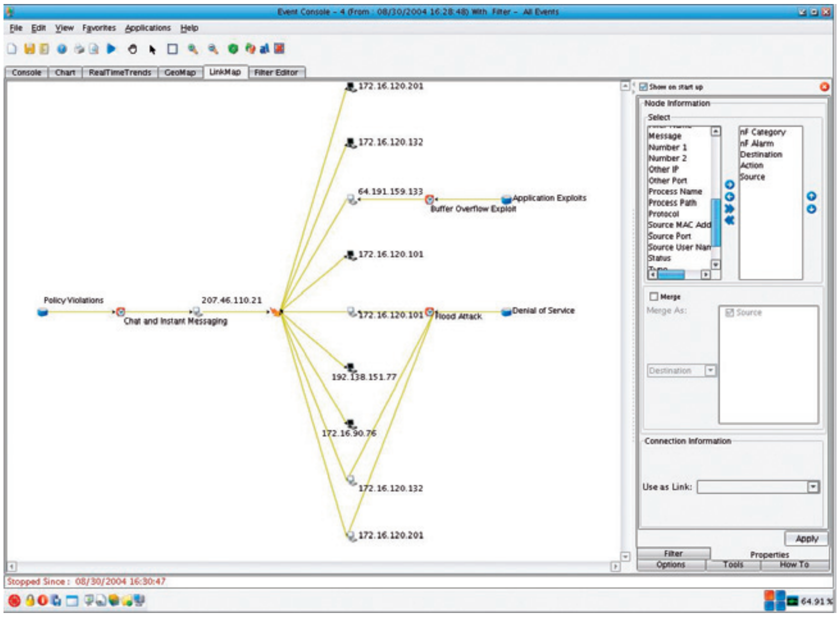
netForensics Open Security Platform provides users with multiple views of information that are tightly integrated with reporting and analytics to intuitively pinpoint threats.

GEO MAP—Allows analysts and operators to track events by country and city, flag suspicious traffic from specific countries, and pinpoint suspicious sources down to a specific longitude and latitude.

INTERACTIVE CHARTS—Give users more visual references that are easy to understand. Users have a wide range of custom charting options to help identify threats and present summary views of data to management. Charts are fully drillable, creating links for further exploration.

THE DEVICE STATUS VIEW—Creates real-time visibility into the status of devices across the network, making device count charts easier to view and analyze. The device status view also enables centralized configuration of devices.

INTEGRATED RESOLUTION MANAGEMENT—Users can attach specific Link Map, Geo Map and Chart Views to incident cases so different members of the security team can replicate the threat identification process throughout the remediation lifecycle.



The Link Map allows analysts to identify a threat source as well as all potentially infected machines.

Incident Resolution Management

netForensics' nFX Open Security Platform delivers all of the data and procedural information necessary to resolve even the most complex security incidents. nFX OSP's incident resolution management capabilities focus on gathering and organizing security event data into a logical form and then enforcing a proper security response workflow in order to facilitate a fast and effective response to security incidents.

The nFX Open Security Platform features one of the most advanced security incident resolution management solutions available today, offering a complete range of features to handle even the most complex security incident management needs. The following are some of the key incident management features and benefits of the nFX Open Security Platform:

INTUITIVE AND EASY TO USE GRAPHICAL USER INTERFACE—nFX OSP uses a powerful, yet easy to use graphical user interface (GUI). From the GUI, operators and analysts can easily open, edit, and close security incidents. Using the intuitive interface, users are guided through the steps necessary to create and resolve virtually any security incident. nFX OSP allows analysts to open cases based on the observed real-time events, historical events revealed by forensics reports, or other incident indicators in use within a customer's enterprise.

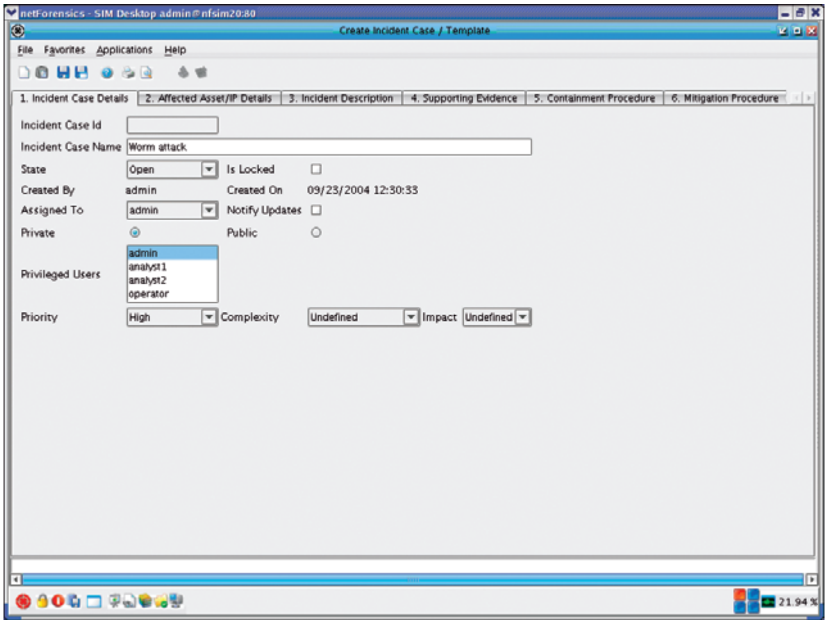
BUILT-IN WORKFLOW—nFX Open Security Platform integrates the SANS* Institute six-step incident response process. By utilizing this flexible, comprehensive, and customizable workflow, users are assured that each security incident is handled with a rigorous, defined, documented, and complete process that is targeted specifically at security incidents. Additionally, nFX OSP offers pre-configured incident templates and site-customizable incident resolution management procedures, which simplify the incident resolution management process. This allows organizations to tailor the out-of-the-box workflow to address the unique process requirements as defined in their incident resolution plan.

*For more information about SANS Institute best practices, please visit www.sans.org.

BUILT-IN KNOWLEDGE BASE—An integrated knowledge base offers vendor-specific device information as well as a complete database of security best practices from sources such as CERT and CVE, as well as supported device vendors. With an in-depth warehouse of security information at their fingertips, operators and analysts command powerful decision support capabilities that, in turn, make incident response a much easier and more streamlined process.

EVIDENCE RETENTION & SECURITY—Virtually any document, image, report, chart or other relevant data can be attached to an individual incident case. Other files, such as scanned images, audio interview records and traffic captures may be also added to cases and will be cryptographically check summed upon insertion to assure the integrity of evidence. Different authorized users may also add notes and comments to the case to alert others and to cover additional aspects of the investigation.

ROLE-BASED ACCESS, INCIDENT COLLABORATION, & INCIDENT SECURITY—nFX OSP cases may be assigned to different system users as well as shared among a group of users. Case change notification is both flexible and configurable. Granular access controls are applied to case data and incident management system functionality, so that several analysts may collaborate on a case while maintaining important "need to know" authorization structures. This key feature provides a secure way to store case evidence and apply tight and granular access controls to case data, while still allowing investigators to work together on a case. Additionally, all actions performed by the system users on the case are recorded in the audit log. Finally, when the investigation is concluded, the case handler may choose to export the case to other systems. Final reports include all case data and may be printed or sent by email.


netForensics - SIM Desktop admin@nfsim20:80
Create Incident Case / Template
File Favorites Applications Help
1. Incident Case Details
2. Affected Asset/IP Details
3. Incident Description
4. Supporting Evidence
5. Containment Procedure
6. Mitigation Procedure
21.94 %

Incident Case Id
Incident Case Name: Worm attack
State: Open Is Locked ☐
Created By: admin Created On: 09/23/2004 12:30:33
Assigned To: admin Notify Updates ☐
Private ● Public ○
Privileged Users: admin, analyst1, analyst2, operator
Priority: High Complexity: Undefined Impact: Undefined

A comprehensive incident resolution management workflow is available from anywhere in the nFX Open Security Platform.

REPORTING—Robust reporting capabilities include both incident level and executive level reports. Incident cases can be easily searched by authorized operators and analysts from within the incident case database. Case reports can be generated on individual cases or groups of cases. For management and executives, case monitoring and summary reports are easily generated. Additionally, nFX OSP can be configured to automatically generate incident reports to share with company management or third parties.

INTEGRATED THREAT VISUALIZATION—Users can attach specific Link Map, Geo Map and Chart views to cases so different members of the security team can replicate the threat identification process throughout the remediation life cycle.

UNIFIED POLICY COMPLIANCE & REMEDIATION—nFX OSP takes information related to policy violations and closes the loop by triggering a workflow that allows teams to contain and remedy any policy violations that represent real network attacks. nFX OSP simultaneously ensures that vulnerable systems apply appropriate updates and definitions so the network can be accessed safely.

REMEDY® INTEGRATION—In addition to providing a security specific workflow as part of the SIM environment, nFX Open Security Platform's incident resolution management process integrates with Remedy® to facilitate communication with other IT groups like network operations that are involved in the remediation process.

Policy Compliance

netForensics is the first SIM vendor to introduce real-time security policy compliance reporting to ensure that devices and users accessing the network comply with established security policies:

PRE-EMPTIVE POLICY COMPLIANCE—nFX OSP can detect policy violations and then perform comprehensive correlation and forensic analysis to determine whether the presence of multiple policy violations indicates a wider attack. Most importantly, when implemented as part of an integrated policy compliance directive such as Cisco's Network Admission Control (NAC) initiative, this information can be used to deny vulnerable machines access to the network until the appropriate patches and updates have taken place. Finally, violation information can be attached to an incident case to close the loop. nFX OSP then facilitates a remediation workflow to bring vulnerable, non-compliant systems up to operational standards.

Vulnerability Management

nFX OSP helps organizations derive more value from their SIM investment by delivering core vulnerability management functionality to help security teams actively identify asset weaknesses before they can be exploited, and facilitating remediation procedures:

ADVANCED VULNERABILITY REPORTING —Allows the security organization to demonstrate progress in eliminating vulnerabilities that relate to key business objectives like policy compliance. This also aids the development and revision of mitigation and policy compliance strategies. Vulnerability reports can be scheduled for delivery or viewed as part of a security or executive dashboard.

RISK SCORING—Prioritizes threats based on asset value so analysts can take action on threats with the most loss potential for the organization first. This is a powerful complement to vulnerability correlation, and is important for making key vulnerability data valuable.

VULNERABILITY SCANNER INTEGRATION—Incorporates data from vulnerability scanners to provide an up-to-date picture of vulnerable assets. The nFX Open Security Platform integrates with leading vulnerability scanners including eEye Retina Scanner, Foundstone Scanner, Harris Stat Scanner Professional Edition, ISS Internet Scanner, andNessus Scanner.

RESOLUTION PROCEDURES—Walk security analysts through the process of fixing specific vulnerabilities so no steps are missed. A library of procedures is available from the knowledge base, so analysts and operators have specific mitigation information for vulnerabilities at their fingertips throughout the incident resolution process.

DYNAMIC KNOWLEDGE BASE—Contains updated security information on known vulnerabilities, including a database of known vulnerabilities that can be correlated against scanner data, as well as published advisories on new vulnerabilities that are updated monthly. These advisories not only educate analysts on the vulnerabilities, but show how to best use nFX OSP to pinpoint the vulnerabilities. Analysts can access the knowledge base from any point within the nFX Open Security Platform, saving hours of research time and improving responsiveness.

About netForensics

netForensics is the leading authority in Security Information Management (SIM) with more than 300 clients—including Global 1000 enterprises and government organizations operating some of the largest networks in the world. netForensics is the only SIM vendor with an integrated family of enterprise-class products and services that are based on the proven, repeatable nFX information security methodology. This combination empowers security organizations to combat threats more efficiently, while connecting the security organization with network operations, compliance, and risk management. With award-winning technology, netForensics improves security operations performance by extracting real-time intelligence from point security products and applications into a single data repository, flagging the most-critical issues and launching integrated incident resolution and remediation processes.